REMARKS

Claims 1-10, 12, 13, 15-17, 19, 21 and 22 are currently pending in the subject application and are presently under consideration. Claim 15 has been amended as shown at page 4 of the Reply to include previously presented limitations from independent claim 1. Entry of this amendment is respectfully requested as it does not constitute a new limitation that would require a new search.

Applicants' representative thanks Examiners for the courtesies extended during the telephonic interviews conducted on June 20, 2007. Examiners wer contacted to discuss the claim rejections under 35 U.S.C. §112 and 35 U.S.C. §103(a). During the interview it was suggested that applicant's representative identify examples in the specification in support of the argument to overcome the rejection under 35 U.S.C. §112 identified in the Office Action. No agreement was reached regarding the novelty of the subject claims with respect to the cited references under 35 U.S.C. §103(a). Examiners indicated that further search and consideration was required to determine if the claims would be allowed over the cited prior art.

Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

I. Rejection of Claims 1, 12, 21 and 22 Under 35 U.S.C §112

Claims 1, 12, 21 and 22 stand rejected under 35 U.S.C §112, first paragraph, as failing to comply with the enablement requirement. The Office Action asserts that claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. Specifically, the Office Action believes the term "automatically" is unclear as recited in the limitation. However, applicant's representative believes that the Examiner is misinterpreting the term "automatically" to mean "immediately". The term "automatically" means that no manual intervention is required to perform the function, which is the well known meaning of the term to those skilled in the art. (*See e.g.*, page 2, lines 8-21) Therefore, the term is clear as used within claims 1, 12, 21 and 22. As such, this rejection should be withdrawn.

II. Rejection of Claims 1-3, 21 and 22 Under 35 U.S.C. §103(a)

Claims 1-3, 21 and 22 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Tsui (US 2005/0063338) in view of Muratov, *et al.* (US 2003/0097596). It is respectfully submitted that this rejection should be withdrawn for at least the following reasons. Tsui in view of Muratov, *et al.* does not teach each and every element of applicants' invention as recited in the subject claims.

> To reject claims in an application under §103, an examiner must establish a *prima facie* case of obviousness. A *prima facie* case of obviousness is established by a showing of three basic criteria. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *See* MPEP §706.02(j). The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *See In re Vaeck,* 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

The subject claims relates to identification of the type of security employed on a wireless network by detecting failures and timeouts during authentication. By recognizing failures or timeouts during particular portions of the authentication process, an iterative approach can narrow down the possible encryption types until identification of the encryption type being employed is achieved, without any user input or pre-stored information regarding the network encryption type. In particular, independent claim 1 (and similarly independent claims 21 and 22) recites *a detection component that automatically identifies an encryption type of an available wireless network, wherein* ***identification of the encryption type is based at least in part upon a failure of a portion of an authentication sequence or exceeding a time threshold during the authentication sequence***.

As conceded in the Office Action dated May 31, 2007, Tsui does not teach or suggest the aforementioned novel features as recited in the subject claims. The cited reference discloses a system for switching between available wireless networks when roaming based on added

benefits such as better signal strength or faster network. The system employs beacon information received/downloaded from the network to identify the network type. A code is downloaded from the beacon indicating the network protocol. The cited reference relies upon the beacon providing the network identifying information. Any information regarding the network is based upon pre-stored information that has been entered in advance by someone that is then downloaded when needed. Furthermore, the cited reference fails to discuss encryption types being employed on a wireless network. Tsui fails to disclose any methods that do not require some pre-stored information about the network type. Tsui is silent regarding recognition of failures or timeouts during authentication in order to determine the encryption type being employed in the network. Muratov, *et al.* is cited to makeup for the aforementioned deficiencies of Tsui. However, Muratov, *et al.* also fails to teach the above noted novel features of the subject claims. The cited reference teaches a multi-layered security system for a PDA that employs a password, encrypted data, and data-erasing. A password is requested and if the password is correctly entered then data is decrypted when requested by the user. If an incorrect password is entered a certain number of times then the data is erased. The Office Action asserts that failure to enter the correct password is equivalent to determining the encryption type of a wireless network. On the contrary, the cited reference fails to discuss any encryption types used for authentication, such as WEP, WAP, or 802.1x and also fails to teach determining encryption type. It merely discloses checking whether a user entered password is correct or incorrect, which is not equivalent to determining encryption type for a wireless network. Therefore, Tsui in view of Muratov, *et al.* fails to teach or suggest a detection component that identifies an encryption type of an available wireless network, wherein identification of the encryption type is based at least in part upon a failure of a portion of an authentication sequence or exceeding a time threshold during the authentication sequence.

In view of the foregoing, applicants' representative respectfully submits that Tsui and Muratov, *et al.*, alone or in combination, fails to teach or suggest all limitations of independent claims 1, 21, and 22 (and claims 2-3 that depend there from), and thus fails to make obvious the subject claims. Accordingly, withdrawal of this rejection is respectfully requested.

III. Rejection of Claims 1, 4-10, 12, 13 and 19 Under 35 U.S.C. §103(a)

Claims 1, 4-10, 12, 13 and 19 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Fascenda (US 2004/0068653) in view of Muratov, et al. (US 2003/0097596). It is respectfully submitted that this rejection should be withdrawn for at least the following reasons. Fascenda in view of Muratov, *et al.* does not teach each and every element of applicants' invention as recited in the subject claims.

Independent claim 1 (and similarly independent claims 12 and 19) recites *a detection component that automatically identifies an encryption type of an available wireless network, wherein* ***identification of the encryption type is based at least in part upon a failure of a portion of an authentication sequence or exceeding a time threshold during the authentication sequence.*** As conceded in the Office Action dated May 31, 2007, Fascenda does not teach or suggest the aforementioned novel features as recited in the subject claims. The cited reference discloses a system employing access keys to authenticate users to a network. In particular, access keys are stored on a client machine for each network to which the client machine will make a connection. The reference discloses that the access key along with accompanying network information is populated by an administrator or user in advance of connecting to a network. In order to identify a network, the BSSID of the network access point is employed. The BSSID is matched up with the appropriate access key and network information stored on the client machine. Fascenda relies upon the unique BSSID and pre-stored access key information to accomplish identification of the encryption type of the network. Fascenda, like Tsui, is silent regarding recognition of failures or timeouts during authentication in order to determine the encryption type being employed in the network. During the telephonic interview paragraph [0061] of Fascenda was mentioned as possibly anticipating this novel feature. However, this section of Fascenda merely discloses that if the user attempts to connect to a network and the access key does not match, the access key may be associated with another network. The administrator would then have to manually populate any network type information associated with access key. Muratov, *et al.* is cited to makeup for the aforementioned deficiencies of Fascenda. However, as discussed above in section (II), Muratov, *et al.* also fails to teach that identification of the encryption type is based at least in part upon a failure of a portion of an authentication sequence or exceeding a time threshold during the authentication sequence. Muratov, *et al.* merely discloses checking whether a user entered password is correct or

incorrect, which is not equivalent to determining encryption type for a wireless network. Muratov, *et al.* fails to discuss encryption types and Fascenda only suggests using pre-stored information regarding the network. Therefore, Fascenda in view of Muratov, *et al.* fails to teach or suggest a detection component that identifies an encryption type of an available wireless network, wherein identification of the encryption type is based at least in part upon a failure of a portion of an authentication sequence or exceeding a time threshold during the authentication sequence.

In view of the foregoing, applicants' representative respectfully submits that Fascenda and Muratov, *et al.*, alone or in combination, fails to teach or suggest all limitations of independent claims 1, 12, and 19 (and claims 4-10 and 13 that depend there from), and thus fails to make obvious the subject claims. Accordingly, withdrawal of this rejection is respectfully requested.

IV. Rejection of Claims 15-17 Under 35 U.S.C. §103(a)

Claims 15-17 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Fascenda (US 2004/0068653) in view of Balogh (US 2001/0023446). It is respectfully submitted that this rejection should be withdrawn for at least the following reasons. Fascenda in view of Balogh does not teach each and every element of applicants' invention as recited in the subject claims.

Independent claim 15 recites ***determining whether a wireless network supports 802.1x based at least in part upon a failure of a portion of an authentication sequence or exceeding a time threshold during the authentication sequence; identifying the wireless network as an wired equivalent privacy network requiring a wired equivalent privacy key, if the wireless network does not support 802.1x. determining whether the wireless network supports wireless provisioning services if the wireless network supports 802.1x based at least in part upon a failure of a portion of an authentication sequence or exceeding a time threshold during the authentication sequence; and, identifying the wireless network as an 802.1x network, if the wireless network does not supporting wireless provisioning services; and, identifying the wireless network as a wireless provisioning services supporting network, if the wireless network supports wireless provisioning services.*** The subject claim discloses a sequential approach wherein failure of identification of one type of network is indicative of another network

type. As conceded in the Office Action, Fascenda does not disclose the novel features of this claim. As discussed above, Fascenda relies on a BSSID and pre-stored user populated network identification information associated with the BSSID for identification of network type. Fascenda fails to disclose an iterative approach as recited in the subject claim for identification of the network and encryption type. Balogh is cited to makeup for the aforementioned deficiencies of Fascenda. However, Balogh also fails to teach the above noted novel features of the subject claims. The Office Action asserts that scanning for networks as taught by Balogh is equivalent to the iterative steps disclosed in the subject claim. On the contrary, Balogh merely discloses that scanning of networks is used to identify network names or network IDs which are then used to match information sets that have been pre-stored with the network setting by a network administrator for each known network. The user can then select the correct information set when connecting the network. Both Fasencda and Balogh rely upon information that has been stored in advance regarding the network type. The subject claim does not rely upon pre-populated information about the network to determine the network authentication type being employed. The subject claim discloses a specific narrowing sequence that checks for various network authentication types in sequential order until the authentication type of the network is identified. Therefore, Fascenda and Balogh fail to teach or suggest determining whether a wireless network supports 802.1x based at least in part upon a failure of a portion of an authentication sequence or exceeding a time threshold during the authentication sequence; identifying the wireless network as an wired equivalent privacy network requiring a wired equivalent privacy key, if the wireless network does not support 802.1x. determining whether the wireless network supports wireless provisioning services if the wireless network supports 802.1x based at least in part upon a failure of a portion of an authentication sequence or exceeding a time threshold during the authentication sequence; and, identifying the wireless network as an 802.1x network, if the wireless network does not supporting wireless provisioning services; and, identifying the wireless network as a wireless provisioning services supporting network, if the wireless network supports wireless provisioning services.

In view of the foregoing, applicants' representative respectfully submits that Fascenda and Balogh, alone or in combination, fail to teach or suggest all limitations of independent claim 15 (and claims 16 and 17 that depend there from), and thus fails to make obvious the subject claimed invention. Accordingly, this rejection should be withdrawn.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [MSFTP552US].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicants' undersigned representative at the telephone number below.

Respectfully submitted,

AMIN, TUROCY & CALVIN, LLP

/Himanshu S. Amin/
Himanshu S. Amin
Reg. No. 40,894

AMIN, TUROCY & CALVIN, LLP
24TH Floor, National City Center
1900 E. 9TH Street
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731